SECUREDA

システム管理者用
運用マニュアル

［第 2 版］

お使いになる前に

この度は、「SECUREDA」をお買いあげいただき、誠にありがとうございます。この取扱説明書は、システム管理者向けの説明書となっており、SECUREDA の機能、設定から運用方法までを解説いたします。

重要なお知らせ（注意事項）

- SECUREDA のご利用の前に、本書および使用許諾書の内容をご確認の上、正しくお使いください。
- SECUREDA は簡易的なシステム制限を行うソフトウェアであり、完全なセキュリティを保障するものではありません。従いまして、SECUREDA を利用したことによる、いかなる損害に関しても当社は責任を負いかねますので、予めご了承ください。
- SECUREDA は、終日稼働するような PC での使用には対応しておりません。
- 制限を適用する PC のユーザーのアカウント種別は、標準ユーザーとすることを検討してください。
- 利用者が持つパソコンの知識によっては、制限を解除されることもございます。
- 利用者により故意に制限を解除しようとすると、動作が不安定になる場合もございます。
- お客様の利用機器・環境等により、制限が有効にならない場合がございます。導入前に、お客様の環境で制限を行えることをご確認ください。
- 本書の内容は、将来予告なしに変更される場合があります。
- 本書の内容の一部、または全部を無断で転載することを禁止します。

他社製品の登録商標および商標についてのお知らせ

☐ Microsoft、Windows は米国 Microsoft Corp.の登録商標です。

☐ その他、各会社名、各製品名は、各社の商標または登録商標です。

目次

SECUREDA とは

「SECUREDA」は、PC 環境に一定の制限を適用することにより、情報の流出を防ぐセキュリティソフトウェア群です。SECUREDA を導入することにより、次のような運用を可能とします。

- PC の資産情報を管理・取得します。
- 周辺機器などの接続を制限し、情報の流出を防ぎます。
- 指定条件に一致したアプリケーションの起動を阻止します。
- 指定した文字列を含むファイル名のファイルアクセスを禁止します。
- 指定したグループの印刷を制限します。

「SECUREDA」は、次の 2 つのソフトウェアで構成されています。

- 制限内容を編集・管理する「DA 管理コンソール」
- 制限をシステム環境に適用・維持する「SECUREDA クライアント」

システム管理者が使用するPC（管理者用 PC）で制限内容を作成し、運用システム内の PC（クライアント PC）へ適用することにより、クライアント PC でのハードウェア（デバイス）の使用制限、ソフトウェアの実行制限、ファイルアクセス制限、印刷制限を行います。一度制限を適用すると、新しい制限を適用する、あるいは「SECUREDA クライアント」をアンインストールするまで、システム制限を維持しますので、ネットワークに接続されていないクライアント PC にも制限を適用することができます。

また、「SECUREDA クライアント」はクライアント PC のハードウェア情報、インストールされているアプリケーション、および PC の利用状況を記録します。この記録された情報を「DA 管理コンソール」で、取得・管理することにより、PC の不正利用を監視することができます。

SECUREDA クライアントの動作環境について

SECUREDA クライアントの動作環境は以下のとおりです。

Microsoft® Windows® 7 Professional

Microsoft® Windows® XP Professional Service Pack 3

Microsoft® Windows® Vista Business Service Pack 2

※ DA 管理コンソールの動作環境については、「DA 管理コンソール取扱説明書」を参照してください。

導入前の準備

制限する内容、および管理する環境を決定する

SECUREDA Pro 導入時の最初の手順として、以下の2つがあげられます。

- SECUREDA による制限が必要かどうか、また制限をどこまで適用するかを検討する
- SECUREDA によるクライアントの管理をどのように行うのか、環境を検討する

ここでは上記2つを検討する際に必要な情報として、以下の２点について説明します。

- SECUREDA で適用可能な制限とはなにか
- SECUREDA で管理する環境とはなにか

SECUREDA で適用可能な制限とはなにか

SECUREDA は、ハードウェアやソフトウェアの動作を制限するソフトウェアですが、過度な制限を設定すると、通常業務にまで支障を生じることになります。また運用規則等により、必要とされる制限も異なります。
パソコンの使用状況等に応じて、制限内容を決定することが重要です。

SECUREDA で設定できる制限は、大きく分けて次の４種類となります。

- ハードウェア制限
- ソフトウェア制限
- ファイルアクセス制限
- 印刷制限

SECUREDA で管理する環境とはなにか

「DA 管理コンソール」では、制限設定とグループは 1 対 1 で関連づけられており、グループに登録されているメンバー（クライアント PC）すべてに対し、グループの制限設定を適用することができます。

部署、あるいは PC 利用者の役割等に基づいてグループ分けを行い、グループ毎に適切な制限設定を作成／適用することが出来ます。

＜DA 管理コンソールにおける、制限設定ファイルとグループ・メンバー（クライアント PC）関係図＞

導入の手順

DA 管理コンソールによる制限設定の基本的な手順は以下のとおりです。
各手順における詳細な操作方法については、「DA 管理コンソール取扱説明書」を参照してください。

１. 管理者 PC に「DA 管理コンソール」をインストールする。

2. 「DA 管理コンソール」の設定をする。
※グループ登録を行います。

3. 「DA 管理コンソール」で、制限設定を行う。
※グループ毎の制限設定を行います。

4. クライアント PC に SECUREDA クライアントをインストールする。

５. メンバーの登録を行う（自動登録）。

6. 制限設定をクライアント PC に配信する。
※上記3. で行った制限設定を配信することにより、クライアント PC に制限が適用されます。

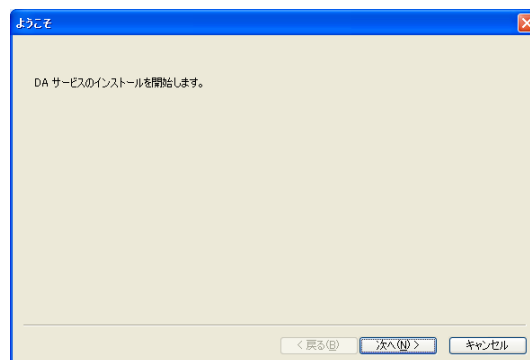
7. クライアント PC から情報を取得し、管理する。

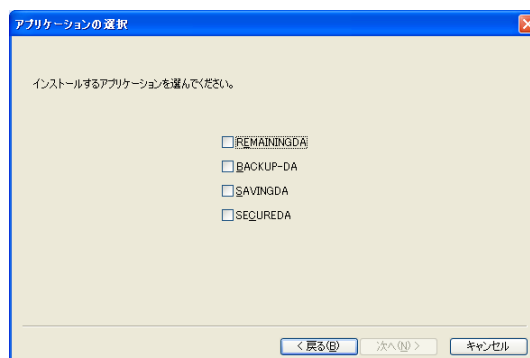
8. 取得した情報をもとに、制限内容および管理環境を見直しする。

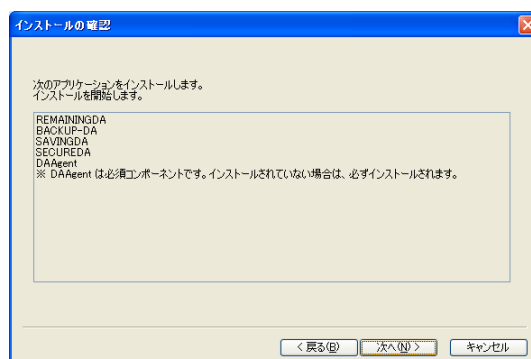
SECUREDA クライアントのインストール

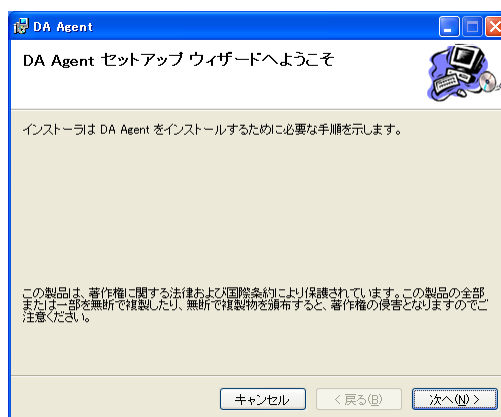
クライアント PC に、「SECUREDA クライアント」をインストールします。

インストールを行う前に、OS が対応 OS であることを確認してください。
また古いバージョンがインストールされている場合、先にアンインストールを行ってください。
※ DA 管理コンソールのインストール手順については、「DA 管理コンソール取扱説明書」を参照してください。

1. クライアント PC で、インストール CD の“Client”フォルダにある“DASetup.exe”を実行してください。
2. DA サービスのインストールとなります。次の画面が表示されたら、「次へ」を押してください。

＜インストーラ起動時画面＞

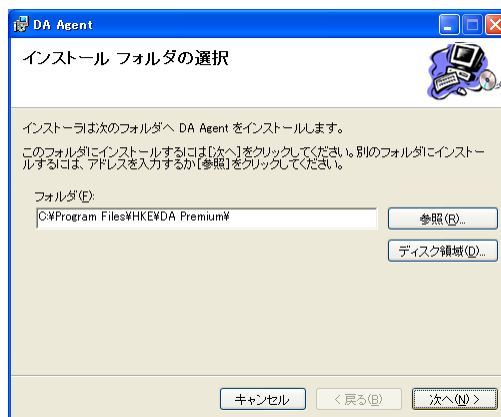
3. （DA Premium インストール時のみ）インストールするアプリケーションの選択画面を表示します。次の画面が表示されたら、SECUREDA を選択して「次へ」を押してください。

＜DA 選択画面＞

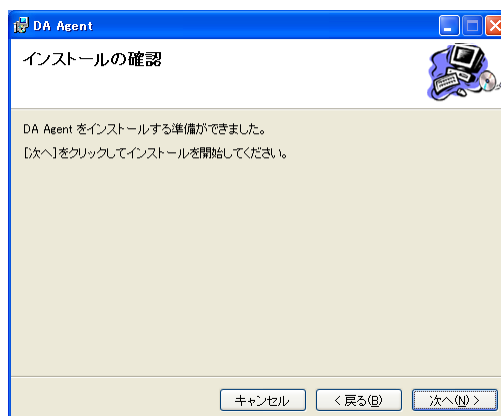
4. インストールの確認画面となります。確認したら、「次へ」を押してください。

＜インストール項目確認画面＞

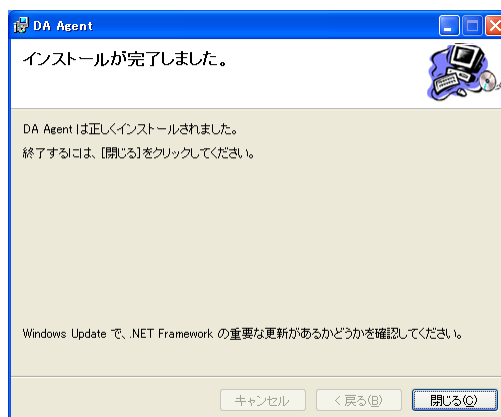
5. インストールの開始画面となります。準備が出来たら、「次へ」を押してください。

＜インストール開始画面＞

6. ネットワークに用いるポート番号を登録する画面が表示されます。
   特に不都合が無い限りポートは初期設定のままで、サーバIPアドレスを入力して「次へ」を押してください。
   他のアプリケーションで使用している場合は、別のポート番号を登録してください。

＜初期設定画面＞

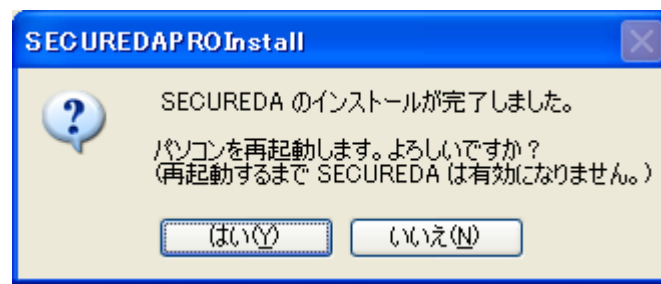
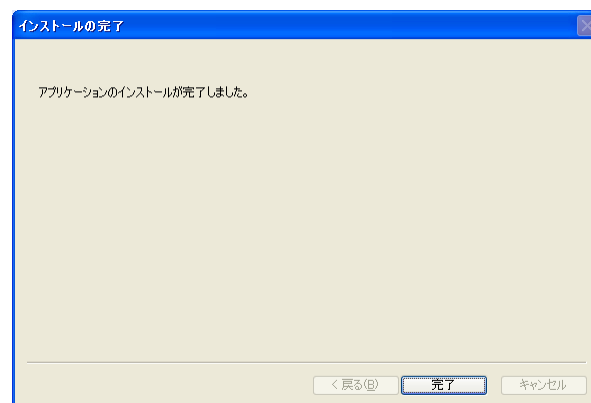
7. インストール先のフォルダを設定する画面が表示されます。
   インストール先のフォルダを変更したい場合は、パスを指定してください。設定が完了したら「次へ」を押してください。

＜インストール フォルダ選択画面＞

8. 下記のインストールの確認を示す画面が表示されますので、「次へ」を押してください。

＜インストールの確認画面＞

9. インストールが完了すると、下記の画面が表示されますので「閉じる」を押して、インストールを終了してください。

＜インストール完了画面＞

10. 次に、SECUREDA クライアントのインストール先を指定する画面が表示されます。
特に不都合が無い限り、デフォルト設定のままで「次へ」を押してください。

＜インストール先指定画面＞

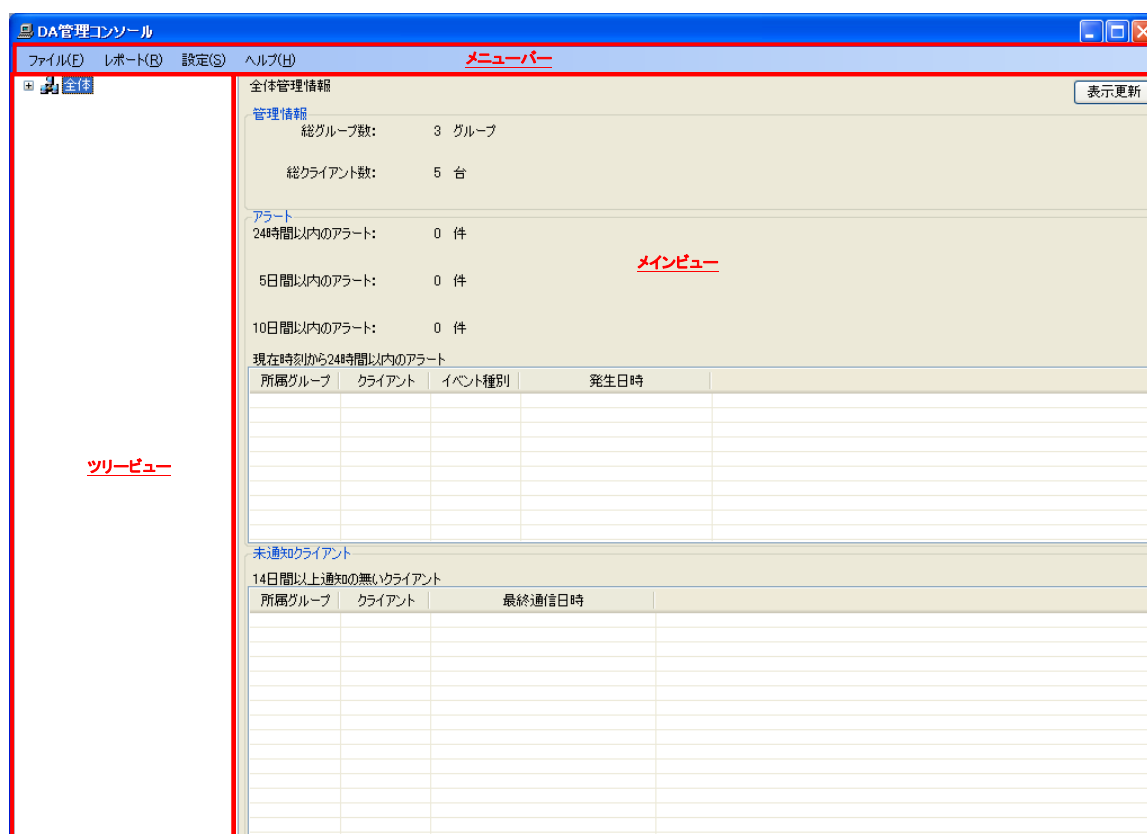
11. SECUREDA クライアントのインストールが完了すると、再起動を促すメッセージが表示されますので、「はい」を押してパソコンを再起動してください。

12. インストールが完了すると、下記の画面が出ますので、「完了」を押して、インストールを終了してください。

資産情報について

ここでは、クライアントの資産情報について説明します。

画面構成

DA 管理コンソールの画面構成を説明します。

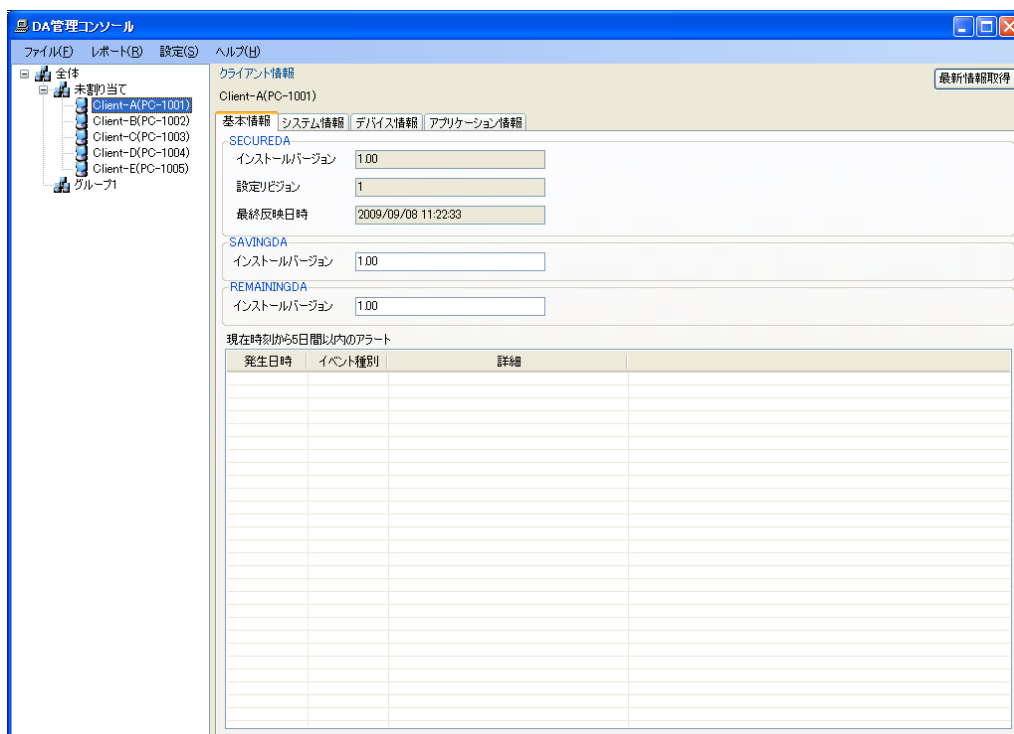
※本説明書では、以後、以下の画面に赤色で示すように、画面左側をツリービュー、右側をメインビュー、画面上部（ファイルやヘルプと表示されている部分）をメニューバーと呼称します。

＜DA 管理コンソール画面＞

基本情報

基本情報には、以下の情報が表示されています。

- SECUREDA のインストールバージョン、設定リビジョン、最終反映日時
- SAVINGDA のインストールバージョン
- REMAININGDA のインストールバージョン
- 現在時刻から5日以内のアラート

ツリービューにて、情報を表示したいクライアントをクリックします。

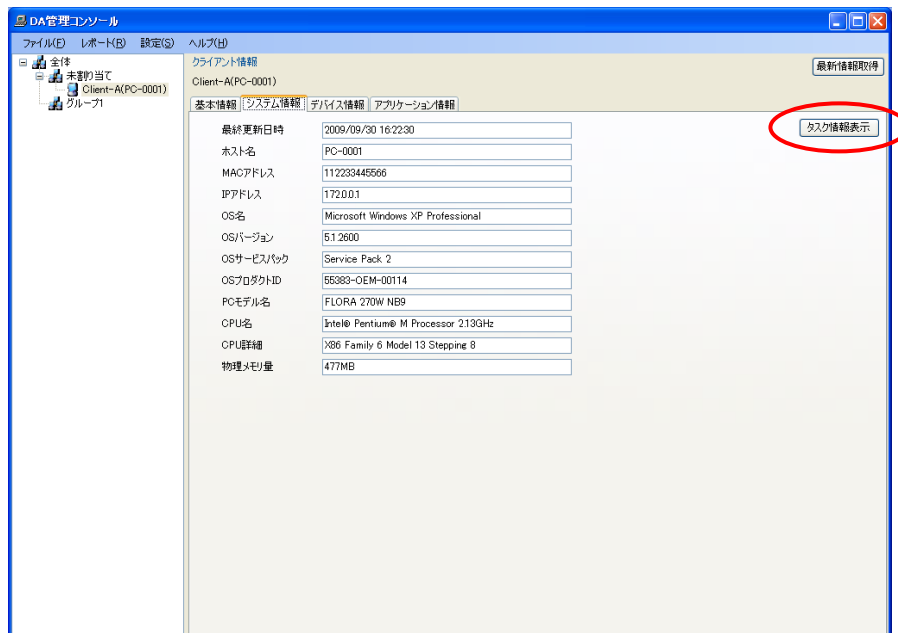
「基本情報」タブをクリックすると、クライアントの基本情報が表示されます。

＜基本情報画面＞

システム情報

システム情報には、以下の情報が表示されています。

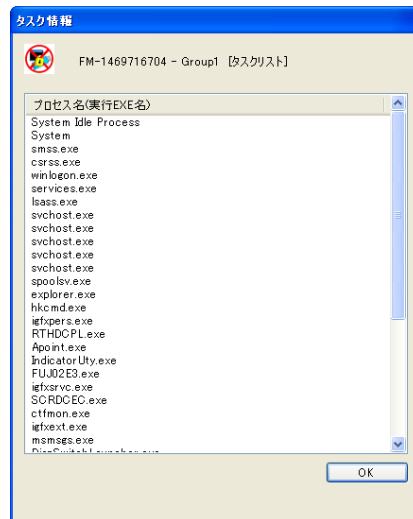
- 最終更新日時
- ホスト名（クライアント PC のフル コンピュータ名）
- MAC アドレス（クライアントPCのMACアドレス）
- IPアドレス（クライアントPCのIPアドレス）
- OS 名（クライアント PC にインストールされている OS の名前）
- OS バージョン（クライアント PC にインストールされている OS のバージョン情報）
- OS サービスパック（クライアント PC にインストールされている OS サービスパックの情報）
- OS プロダクト ID（クライアント PC にインストールされている OS の製品 ID 情報）
- PC モデル名（クライアント PC の製品名）
- CPU 名（クライアント PC に搭載されている CPU の名前）
- CPU 詳細（クライアント PC に搭載されている CPU の詳細）
- 物理メモリ量（クライアント PC に搭載されているメモリの容量）

ツリービューにて、情報を表示したいクライアントをクリックします。

「システム情報」タブをクリックすると、クライアントのシステム情報が表示されます。

＜システム情報画面＞

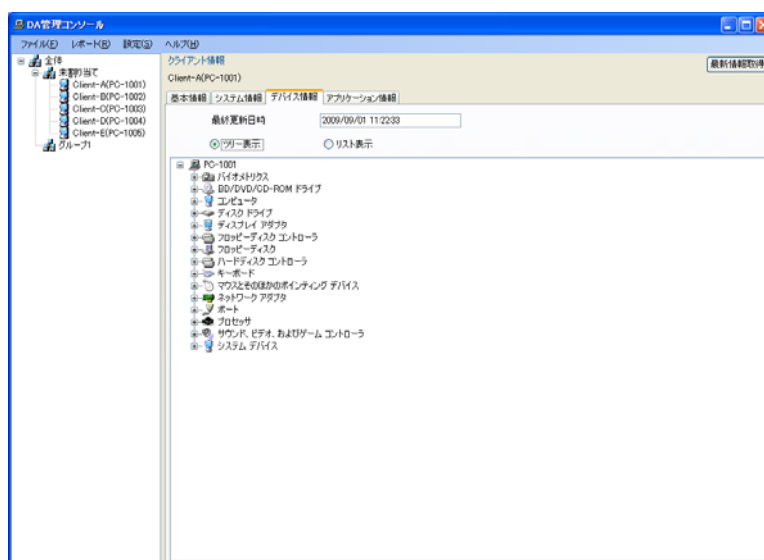
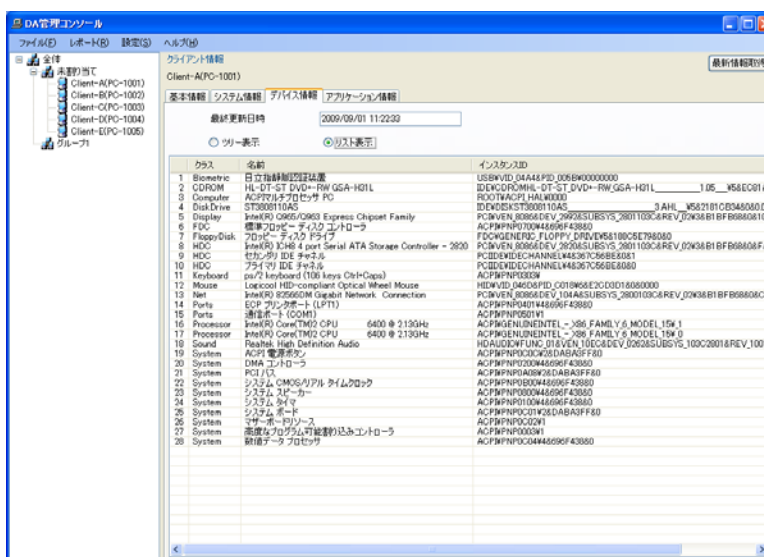
メインビューの画面右上部にある「タスク情報表示」ボタンをクリックすると、タスク情報の表示を行います。

【注意事項】

- タスクリストを取得できるのは、ネットワークに接続しているクライアント PC のみです。
- 取得したタスクリストは、「DA 管理コンソール」から取得した時点のものです。
- 取得したタスクリストは、制限設定更新の目安として利用する機能です。
- 「DA 管理コンソール」は、タスクリストの保存・管理を行いません。

＜タスク情報結果画面＞

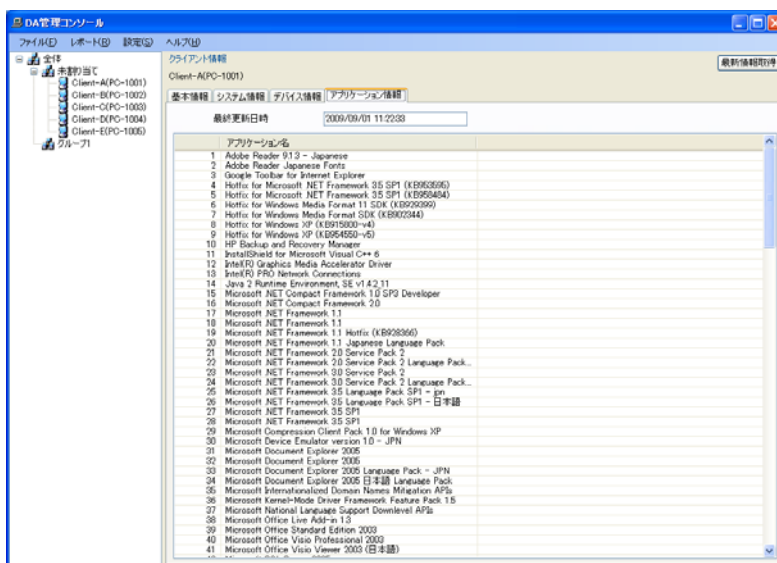
デバイス情報

ハードウェア情報には、クライアント PC が使用しているデバイスの情報が表示されています。この情報は、デバイスマネージャ上で閲覧できる情報と同等のものです。
「DA 管理コンソール」ではハードウェア情報の表示形式として、「ツリー表示」と「リスト表示」の 2 種類を用意してあります。

ツリービューにて、情報を表示したいクライアントをクリックします。
「デバイス情報」タブをクリックすると、クライアントのデバイス情報が表示されます。

＜デバイス情報画面：ツリー表示＞

＜デバイス情報画面：リスト表示＞

アプリケーション情報

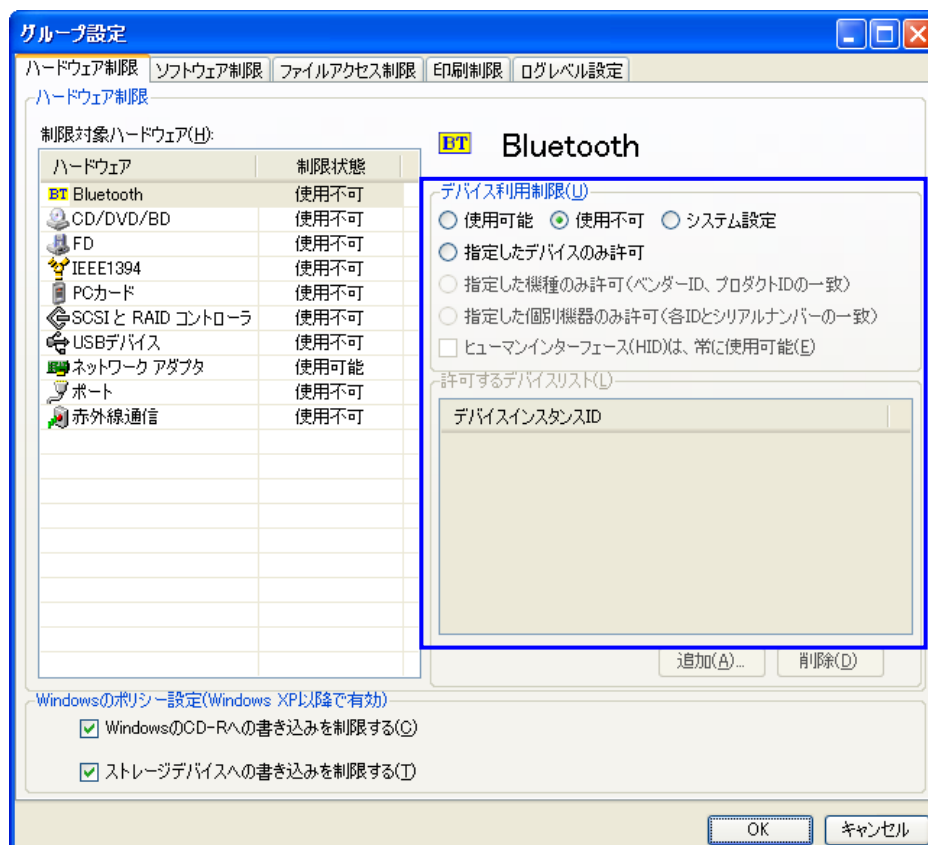
アプリケーション情報には、クライアントPCにインストールされているアプリケーションが表示されます。この情報は、「コントロールパネル」の「プログラムの追加と削除」で表示される内容と同等のものです。

ツリービューにて、情報を表示したいクライアントをクリックします。
「アプリケーションデバイス情報」タブをクリックすると、クライアントのアプリケーションデバイス情報が表示されます。

＜アプリケーション情報画面＞

ハードウェアの利用を制限する

クライアントPCのデバイスを無効化することによって、許可されていない個人所有の機器利用を制限することができます。たとえば、USBメモリ・ポータブルハードディスクドライブなどによる、情報の持出/持込を制限できます。

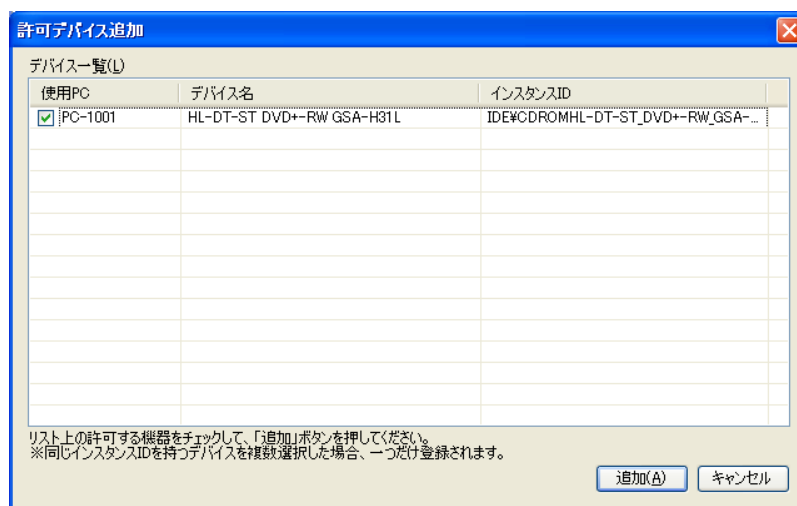
制限方法

1. 管理者用PCのDA管理コンソール上で、「制限設定」ボタンをクリックします。
2. 制限対象ハードウェアの一覧から制限するハードウェアをクリックします。
3. 設定詳細部(□(青四角)で囲まれている部分)が切り替わりますので、それぞれのデバイスに適用したい設定を選択してください。

＜ハードウェア制限画面＞

「指定したデバイスのみ許可」の選択

※CD/DVD/BD・IEEE1394・PC カード・ポート・ネットワークアダプタ・SCSI と RAID コントローラのみ

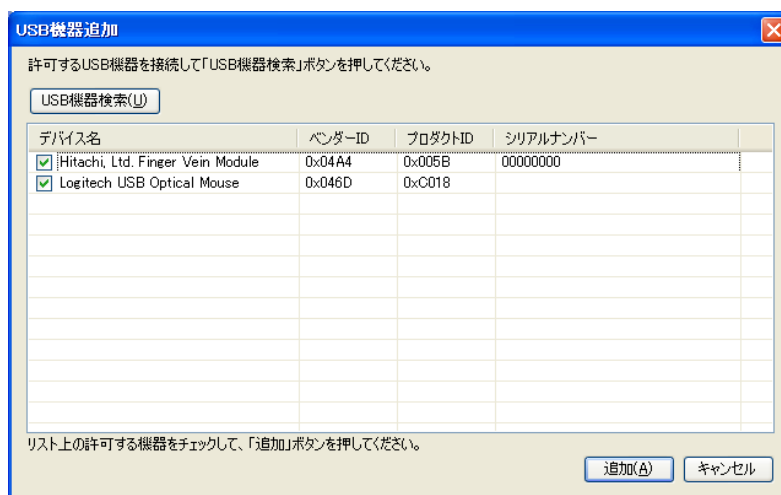
※「指定したデバイスのみ許可」におけるデバイス制限では、予めクライアント PC のハードウェア情報を取得しておく必要があります。クライアント PC から情報を取得する方法については、『DA 管理コンソール取扱説明書』の「8. 制限設定をクライアントPCに配布する」の「クライアントPCから情報を取得する方法」を参照してください。

1. 制限対象ハードウェアの一覧から「デバイス識別」制限が可能なデバイスをクリックします。
2. 口（青四角）で囲まれている部分の表示が切り替わったら、「指定したデバイスのみ許可」を選択します。
3. 設定詳細部の下にある、「追加」ボタンが選択可能になりますので、クリックします。
4. クライアント PC のハードウェア情報がある場合、「追加」ボタンをクリックすると管理しているクライアントPCに接続されているデバイスの一覧がリスト表示されます。使用 PC の欄には、デバイス名の欄に表示されているデバイスを使用しているクライアント PC 名が表示されます。

＜許可デバイス追加画面＞

5. デバイスリストから、使用を許可するデバイスを選択し「追加」ボタンをクリックします。
6. デバイスインスタンス ID リスト内に、選択したデバイスのデバイスインスタンス ID が追加されます。

「指定した機種のみ許可」または「指定した個別機器のみ許可」の選択

※USB デバイスのみ

1. 予め、登録したい USB デバイスを管理者 PC に接続し、利用できる状態にします。
2. メインビューから「USB デバイス」のボタンをクリックします。
3. 口（青四角）で囲まれている部分の表示が切り替わったら、「指定した機種のみ許可」もしくは「指定した個別機器のみ許可」を選択します。
4. 設定詳細部の下にある、「追加」ボタンが選択可能になりますので、クリックします。
5. 「追加」ボタンをクリックすると、以下のような「USB 機器追加」画面が表示されますので、「USB 機器検索」ボタンをクリックしてください。管理者 PC に接続されている USB デバイスが全てリストアップされます。
 ※デバイスによっては、デバイス名が表示されない場合があります。

＜USB 機器追加画面＞

6. リストから、使用を許可したいデバイスを選択し「追加」ボタンをクリックします。
7. デバイスインスタンス ID リストに、選択した USB デバイスのデバイスインスタンス ID が追加されます。

SECUREDA で制限できるデバイスは、下記のとおりです。

<table>
<tr><th>デバイス名称</th><th>制限内容</th></tr>
<tr><td>FD</td><td>フロッピーディスクの利用を制限します。
デバイスマネージャ上で「フロッピーディスクコントローラ(※)」に分類される、すべてのドライブが対象になります。
<table>
<tr><td>使用可能</td><td>デバイスの使用が許可されます</td></tr>
<tr><td>使用不可</td><td>デバイスの使用が禁止されます</td></tr>
<tr><td>システム設定</td><td>システムの設定に依存します</td></tr>
</table></td></tr>
<tr><td>CD/DVD/BD</td><td>CD や DVD や BD の利用を制限します。
デバイスマネージャ上で「DVD/CD-ROM ドライブ(※)」に分類される、すべてのドライブが対象になります。ただし、「指定したデバイスのみ許可」が指定された場合は、すべてのドライブが対象ではなく、許可するデバイスリストで追加したデバイスのみが対象となります。
<table>
<tr><td>使用可能</td><td>デバイスの使用が許可されます</td></tr>
<tr><td>使用不可</td><td>デバイスの使用が禁止されます</td></tr>
<tr><td>システム設定</td><td>システムの設定に依存します</td></tr>
<tr><td>指定したデバイスのみ許可</td><td>許可するデバイスリストで追加したデバイスのみ使用が許可されます</td></tr>
</table></td></tr>
<tr><td>IEEE1394</td><td>IEEE1394 接続機器の利用を制限します。
デバイスマネージャ上で「IEEE1394 バスコントローラ(※)」に接続する、すべてのデバイスが対象になります。ただし、「指定したデバイスのみ許可」が指定された場合は、すべてのデバイスが対象ではなく、許可するデバイスリストで追加したデバイスのみが対象となります。
※IEEE1394 は、「iLink」や「FireWire」と呼ばれる場合があります。
<table>
<tr><td>使用可能</td><td>デバイスの使用が許可されます</td></tr>
<tr><td>使用不可</td><td>デバイスの使用が禁止されます</td></tr>
<tr><td>システム設定</td><td>システムの設定に依存します</td></tr>
<tr><td>指定したデバイスのみ許可</td><td>許可するデバイスリストで追加したデバイスのみ使用が許可されます</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>デバイス名称</th><th>制限内容</th></tr>
<tr><td>PC カード</td><td>PC カード（PCMCIA）の利用を制限します。
デバイスマネージャ上の「PCMCIA アダプタ(※)」に接続する、すべてのデバイスが対象になります。ただし、「指定したデバイスのみ許可」が指定された場合は、すべてのデバイスが対象ではなく、許可するデバイスリストで追加したデバイスのみが対象となります。
<table>
<tr><td>使用可能</td><td>デバイスの使用が許可されます</td></tr>
<tr><td>使用不可</td><td>デバイスの使用が禁止されます</td></tr>
<tr><td>システム設定</td><td>システムの設定に依存します</td></tr>
<tr><td>指定したデバイスのみ許可</td><td>許可するデバイスリストで追加したデバイスのみ使用が許可されます</td></tr>
</table></td></tr>
<tr><td>SCSI と RAID コントローラ</td><td>SCSI アダプタと RAID コントローラの利用を制限します。
デバイスマネージャ上の「SCSI アダプタと RAID コントローラ(※)」に接続する、すべてのデバイスが対象になります。ただし、「指定したデバイスのみ許可」が指定された場合は、すべてのデバイスが対象ではなく、許可するデバイスリストで追加したデバイスのみが対象となります。
<table>
<tr><td>使用可能</td><td>デバイスの使用が許可されます</td></tr>
<tr><td>使用不可</td><td>デバイスの使用が禁止されます</td></tr>
<tr><td>システム設定</td><td>システムの設定に依存します</td></tr>
<tr><td>指定したデバイスのみ許可</td><td>許可するデバイスリストで追加したデバイスのみ使用が許可されます</td></tr>
</table></td></tr>
<tr><td>ポート</td><td>COM ポートや LPT ポートの利用を制限します。
デバイスマネージャ上の「ポート (COM と LTP)(※)」に分類される、すべてのポートが対象になります。ただし、「指定したデバイスのみ許可」が指定された場合は、すべてのポートが対象ではなく、許可するデバイスリストで追加したポートのみが対象となります。
<table>
<tr><td>使用可能</td><td>デバイスの使用が許可されます</td></tr>
<tr><td>使用不可</td><td>デバイスの使用が禁止されます</td></tr>
<tr><td>システム設定</td><td>システムの設定に依存します</td></tr>
<tr><td>指定したデバイスのみ許可</td><td>許可するデバイスリストで追加したデバイスのみ使用が許可されます</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>デバイス名称</th><th>制限内容</th></tr>
<tr><td>赤外線通信</td><td>赤外線通信（IrDA)の利用を制限します。
デバイスマネージャ上の「赤外線通信(※)」に分類される、すべてのデバイスが対象になります。
<table>
<tr><td>使用可能</td><td>デバイスの使用が許可されます</td></tr>
<tr><td>使用不可</td><td>デバイスの使用が禁止されます</td></tr>
<tr><td>システム設定</td><td>システムの設定に依存します</td></tr>
</table></td></tr>
<tr><td>ネットワークアダプタ</td><td>ネットワークアダプタ（LAN)の利用を制限します。
デバイスマネージャ上の「ネットワークアダプタ(※)」に分類される、すべてのデバイスが対象になります。ただし、「指定したデバイスのみ許可」が指定された場合は、すべてのデバイスが対象ではなく、許可するデバイスリストで追加したデバイスのみが対象となります。
<table>
<tr><td>使用可能</td><td>デバイスの使用が許可されます</td></tr>
<tr><td>使用不可</td><td>デバイスの使用が禁止されます</td></tr>
<tr><td>システム設定</td><td>システムの設定に依存します</td></tr>
<tr><td>指定したデバイスのみ許可</td><td>許可するデバイスリストで追加したデバイスのみ使用が許可されます</td></tr>
</table></td></tr>
<tr><td>USB デバイス</td><td>USB 接続機器の利用を制限します。
他のデバイスと異なり、有効／無効／システム設定のほか、機種識別／個別識別を設定することが可能です。（特定の機器・許可された機器のみ有効で、その他機器は利用不可能）
<table>
<tr><td>使用可能</td><td>デバイスの使用が許可されます</td></tr>
<tr><td>使用不可</td><td>デバイスの使用が禁止されます</td></tr>
<tr><td>システム設定</td><td>システムの設定に依存します</td></tr>
<tr><td>指定した機種のみ許可</td><td>ベンダーID、プロダクト ID の一致する機種の使用のみ許可されます</td></tr>
<tr><td>指定した個別機器のみ許可</td><td>ベンダーID、プロダクト ID とシリアルナンバーの一致する個別機器の使用のみ許可されます</td></tr>
<tr><td>ヒューマンインターフェース(HID)は、常に使用可能</td><td>ヒューマンインターフェースデバイス(HID)を無条件に使用許可します</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>デバイス名称</th><th colspan="2">制限内容</th></tr>
<tr><td rowspan="5">Bluetooth</td><td colspan="2">Bluetooth の利用を制限します。
デバイスマネージャ上の「Bluetooth(※)」に分類される、すべてのデバイスが対象になります。ただし、「指定したデバイスのみ許可」が指定された場合は、すべてのデバイスが対象ではなく、許可するデバイスリストで追加したデバイスのみが対象となります。</td></tr>
<tr><td>使用可能</td><td>デバイスの使用が許可されます</td></tr>
<tr><td>使用不可</td><td>デバイスの使用が禁止されます</td></tr>
<tr><td>システム設定</td><td>システムの設定に依存します</td></tr>
<tr><td>指定したデバイスのみ許可</td><td>許可するデバイスリストで追加したデバイスのみ使用が許可されます</td></tr>
</table>

※ OS によっては、デバイスマネージャ上で表記が異なる場合があります。

また SECUREDA では、下記の制限も可能です。

機能名称	制限内容
Windows の CD-R 書き込み機能を制限する	ハードウェア制限における共通の項目です。 Windows エクスプローラによる CD-R への書き込み機能の使用を禁止します。
ストレージデバイスへの書き込みを制限する	ハードウェア制限における共通の項目です。 デバイスマネージャにおいて、大容量記憶装置デバイスと識別される全てのデバイスは、書込み不可能な状態にします。

注） Windows XP 以降でのみ有効な機能です。

【補足説明】

- すべてのハードウェアを使用禁止にした場合、クライアント PC からの出力だけでなく、入力（ファイルコピーなど）も制限されるため、制限設定の変更および解除ができなくなります。従いまして、運用上必要のないハードウェアのみを制限する、あるいは USB の個別識別などを予め設定しておき、管理者がアクセスできる手段を確保した上で制限を行ってください。すべてのハードウェアを使用禁止にする場合は、「SECUREDA 管理用ソフトウェア」付属の、クライアント・アンインストールプログラムを予めクライアント PC にコピーしておく方法をお勧めします。
- ハードウェア制限を行っているクライアント PC では、デバイスマネージャを使用してデバイスを有効化した場合に、システムの動作が不安定になることが予想されます。ハードウェア制限を行う場合は、同時にデバイスマネージャの実行を制限することをお勧めします。デバイスマネージャの実行制限は、ソフトウェア制限の「Microsoft マネージメントコンソール」で制限可能です。
- 「CD-R 書き込み機能を制限する」では Windows エクスプローラによる CD 書込みは制限されますが、ライティングソフトによる CD 書込みは制限できない場合があります。ライティングソフトによる書き込みも同様に制限する場合は、ソフトウェア制限を併用してください。

設定の反映の確認方法

制限したデバイスは、下記の動作となり利用できなくなります。

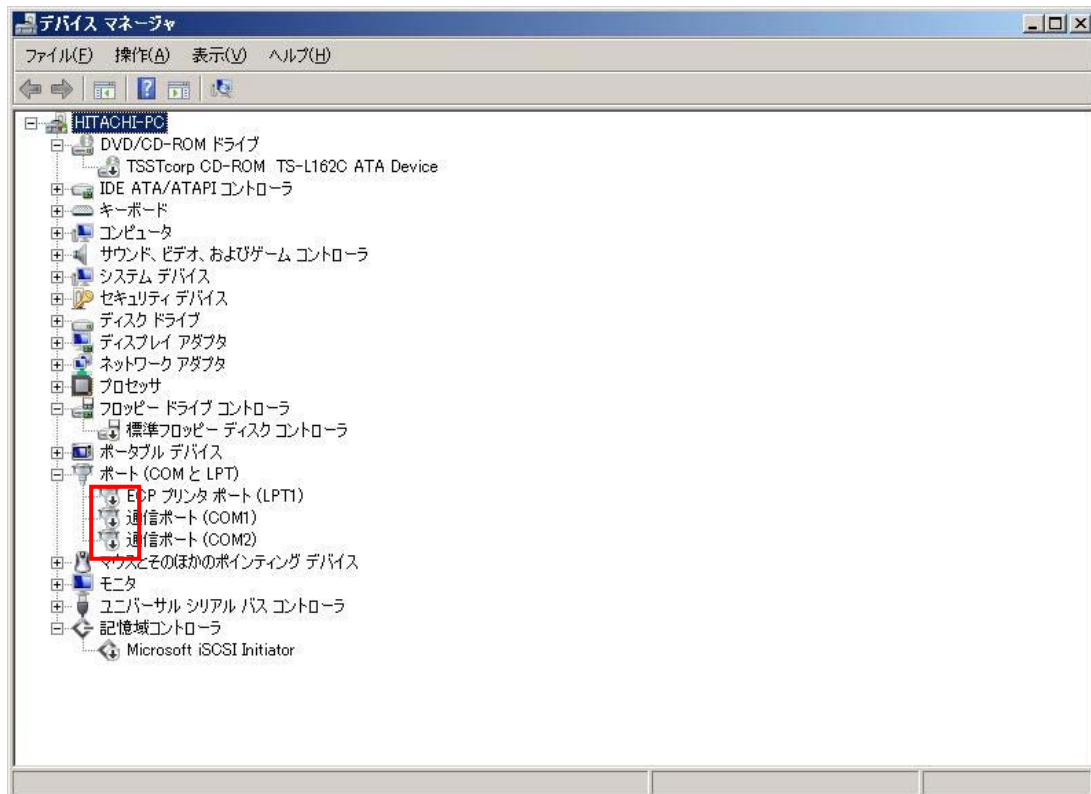
デバイス名称	動作
FD	デバイスマネージャ上で無効になります。
CD/DVD/BD	デバイスマネージャ上で無効になります。
IEEE1394	デバイスマネージャ上で無効になります。
PC カード	デバイスマネージャ上で無効になります。
SCSI と RAID コントローラ	デバイスマネージャ上で無効になります。
ポート	デバイスマネージャ上で無効になります。
赤外線通信	デバイスマネージャ上で無効になります。
ネットワークアダプタ	デバイスマネージャ上で無効になります。
USB デバイス	以下のメッセージを表示して、デバイスは無効となります。 「このデバイスの使用は許可されていません。 詳しくはシステム管理者にお問い合わせください。」 注）デバイスによってはメッセージが出ない場合があります。
Bluetooth	デバイスマネージャ上で無効になります。

機能名称	動作
Windows の CD-R 書き込み機能を制限する	右クリックのコンテキストメニューの「送る」から「DVD/CD-ROM ドライブ(※)」がなくなります。
ストレージデバイスへの書き込みを制限する	書き込みしようとすると、以下のメッセージを表示します。 「このディスクは書き込み禁止になっています。」

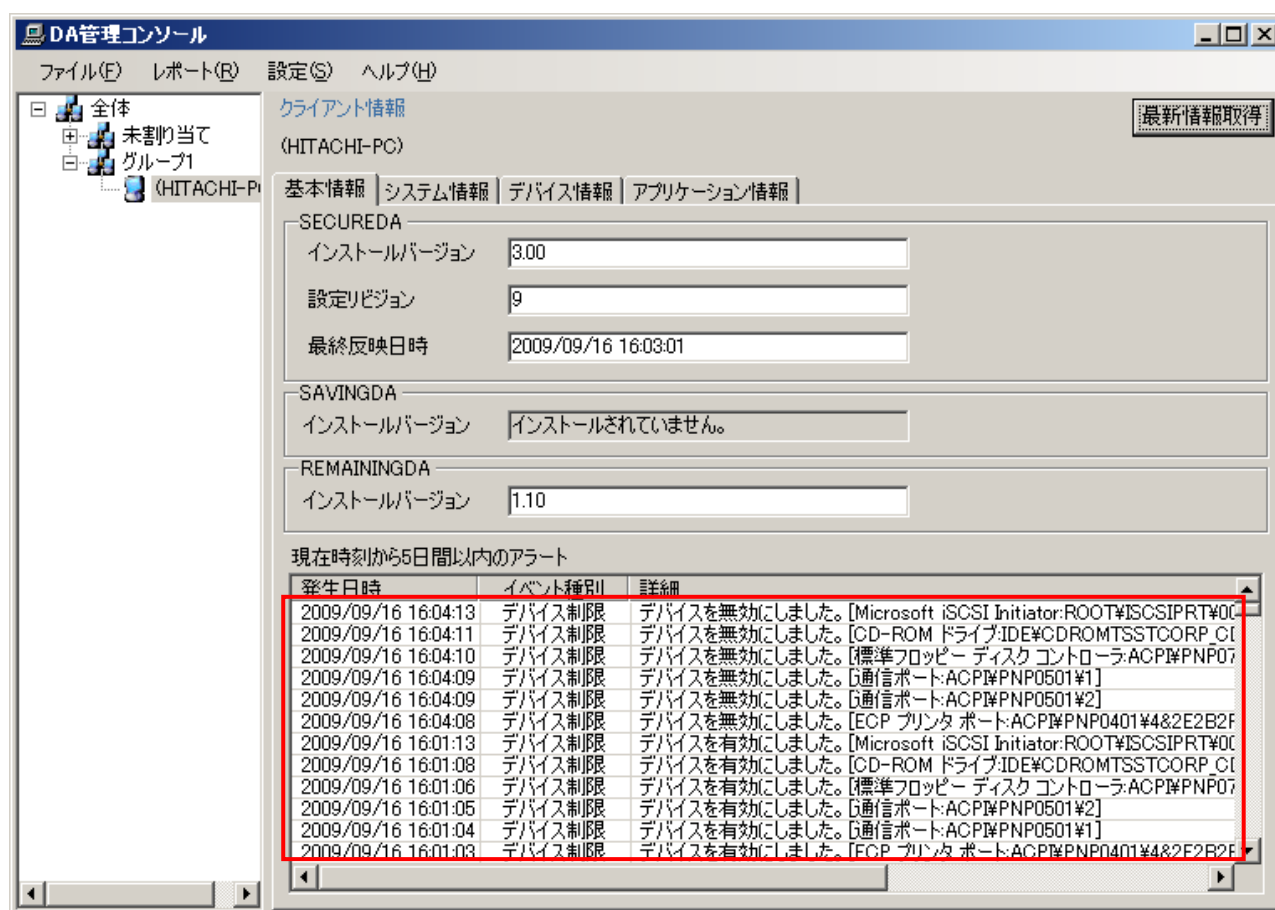
注） Windows XP 以降でのみ有効な機能です。

※ 搭載しているドライブによって表記が異なる場合があります。

[スタート]－[コントロールパネル]から「システム」をダブルクリックして、「ハードウェア」タブから「デバイスマネージャ」ボタンをクリックしてください。

デバイスマネージャ画面を、下記に示します。

＜デバイスマネージャ画面＞

制限結果の確認方法

デバイスを制限すると、管理者用 PC のクライアント情報の「基本情報」画面に以下のように、「デバイスを有効/無効にしました。」とログが出力されます。

＜ハードウェア制限画面＞

メニューバーの「レポート(R)」に結果レポート出力機能をサポートしています。

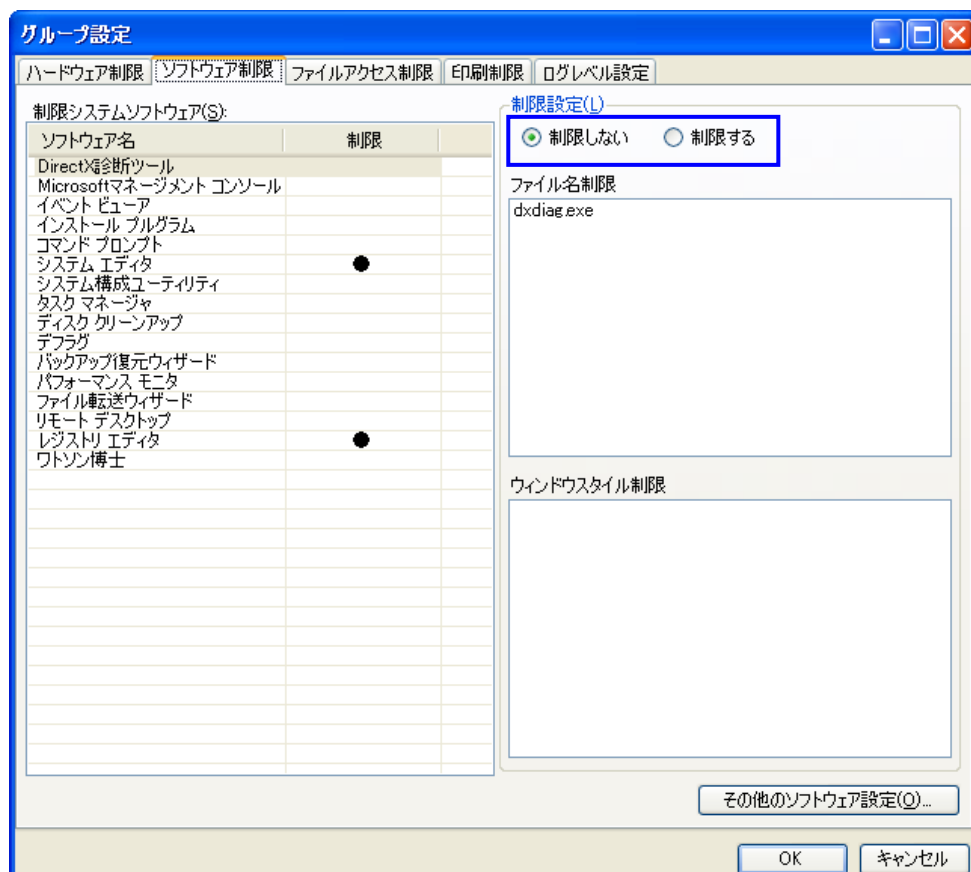
また、CSV 出力機能もサポートしていますので、用途に合わせてご利用ください。

ソフトウェアの利用を制限する

起動ファイル名が一致するソフトウェアの実行と、指定文字列を含むウィンドウタイトルを持つソフトウェアの実行を制限します。

運用上必要のないアプリケーションなどを登録しておき、コンピュータウィルスの感染やスパイウェア等による情報流出を事前に防ぎます。また、システム状態の変更が可能な Windows 標準ソフトウェアの実行を制限することにより、PC 環境の保全、ならびに障害要因を少なくします。

制限方法

1. 制限システムソフトウェアの一覧から制限するソフトウェアをクリックします。
2. 制限設定部（□（青四角））で囲まれている部分）で、適用したい設定を選択してください。
3. 制限したソフトウェアには、●が表示されます。

＜ソフトウェア制限画面＞

SECUREDA には、下記の項目が予め登録されています。

【インストールプログラム】

項目名称	制限内容
インストールプログラム*1	インストール(セットアップ)プログラムの実行を制限します。アプリケーションなどのインストールでよく使用される文字列が登録されています。

【システムプログラム】

項目名称	制限内容
Direct X 診断ツール	Direct X 診断ツールの実行を制限します。
Microsoft マネージメントコンソール	Microsoft マネージメントコンソール（以下、mmc.exe）を利用するアプリケーションの実行を制限します。
イベントビューア	システムイベントを監視するソフトウェアの実行を制限します。
コマンドプロンプト*2	コマンドプロンプトの実行を制限します。
システムエディタ	システムエディタの実行を制限します。
システム構成ユーティリティ	システム構成ユーティリティの実行を制限します。
タスクマネージャ	タスクマネージャの実行を制限します。
ディスククリーンアップ	ディスククリーンアップの実行を制限します。
ディスクデフラグツール	ディスクデフラグツールの実行を制限します。
パフォーマンスモニタ	パフォーマンスモニタの実行を制限します。
リモートデスクトップ	リモートデスクトップ接続の実行を制限します。
レジストリエディタ	レジストリエディタの実行を制限します。
ワトソン博士	ワトソン博士の実行を制限します。

【システムウィザード】

項目名称	制限内容
バックアップ復元ウィザード	バックアップと復元センターの実行を制限します。
ファイル転送ウィザード	ファイル転送ツールの実行を制限します。

【補足説明】

*1:インストールプログラムの制限内容は、インストーラやセットアップで一般的に利用されるファイル名称やウィンドウタイトルが登録されていますが、すべてのインストールプログラムが制限されるわけではありません。また、この制限を適用すると、各種アップデートやブラウザのプラグインのインストールが行えなくなる場合があります。

*2:出荷時設定ではコマンドプロンプトの制限としては、cmd.exe のみが制限されています。COMMAND.COM は内部コマンドとして利用しているアプリケーションがあるため、初期設定では制限から外しています。COMMAND.COM を制限する場合は、新規制限項目として登録を行ってください。

*3：Microsoft マネージメントコンソール（以下、MMC）の実行を禁止すると、MMC を利用するソフトウェア（例：「デバイスマネージャ」、「コンピュータの管理」等）は実行出来なくなります。
*4：パフォーマンスモニタの実行を禁止しても、管理者権限で実行したり、UAC（ユーザアクセス制御）で権限を昇格が行われてしまうと、禁止できません。こうした場合、Microsoft マネージメントコンソールを制限することを検討してください。

【制限する文字列の指定方法について】

ソフトウェア制限では、登録した文字列と、ファイル名/ウィンドウタイトルを比較し制限を行いますが、文字列の指定方法によって比較方法が変わります。SECUREDA でサポートしている指定方法は以下のとおりです。ご利用の環境にあわせて使い分けてください。

比較方法	内容	文字列例(SETUP を制限)
前方一致	ファイル名/ウィンドウタイトルの先頭に指定した文字列を含むアプリケーションを制限します。	setup*
後方一致	ファイル名/ウィンドウタイトルの末尾に指定した文字列を含むアプリケーションを制限します。	*setup
部分一致	ファイル名/ウィンドウタイトルに指定した文字列が含まれるアプリケーションを制限します。	*setup*
完全一致	ファイル名/ウィンドウタイトルが指定した文字と完全に一致するアプリケーションを制限します。	setup

注）エンドユーザーが管理者権限を持っている場合、SECUREDA で完全に制限できない場合があります。

【その他のソフトウェア設定について】

【注意事項】

管理コンソールと、SECUREDAを同じPCにインストールして使われる場合、下記のファイル名や、下記の文字列を含む文字列を制限してしまうと、管理コンソールが起動できなくなってしまいます。

SECUREDA の制限設定も変更できなくなってしまいますので、ご注意ください。

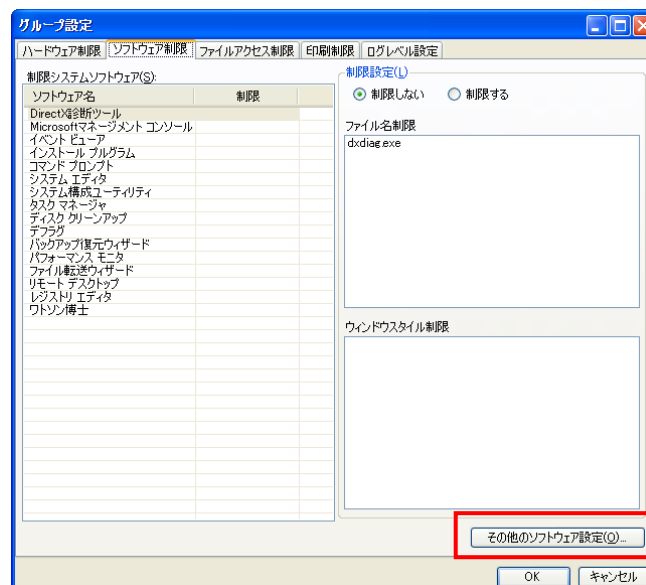
① DAConsole.exe

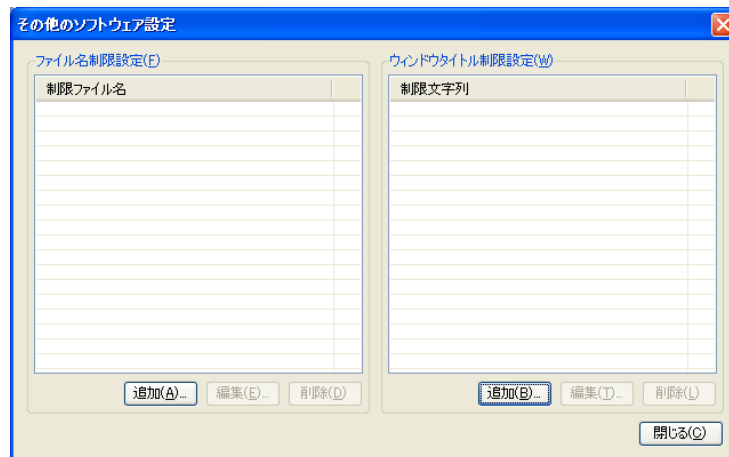
② Manager.exe

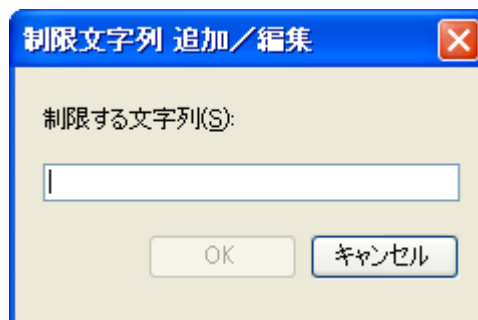
③ Guide.exe

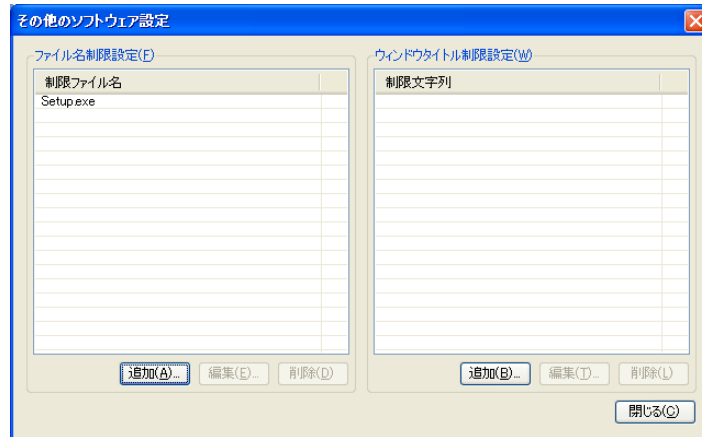
管理コンソールが起動しなくなってしまう設定例：

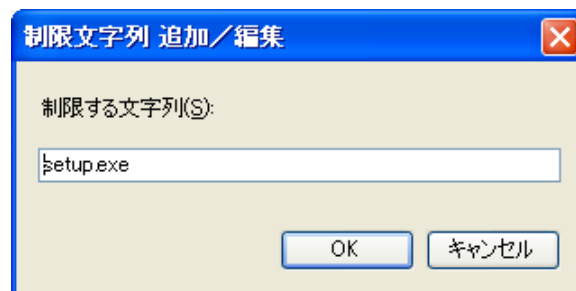
設定した文字列	現象
*Console.exe	“DAConsole.exe”が起動しなくなります。
Man*	“Manager.exe”が起動しなくなります。

1. 管理者用 PC の DA 管理コンソール上で「制限設定」ボタンをクリック、「ソフトウェア制限」タブを選択して、右下部にある「その他のソフトウェア設定」ボタンをクリックします。

＜ソフトウェア制限＞

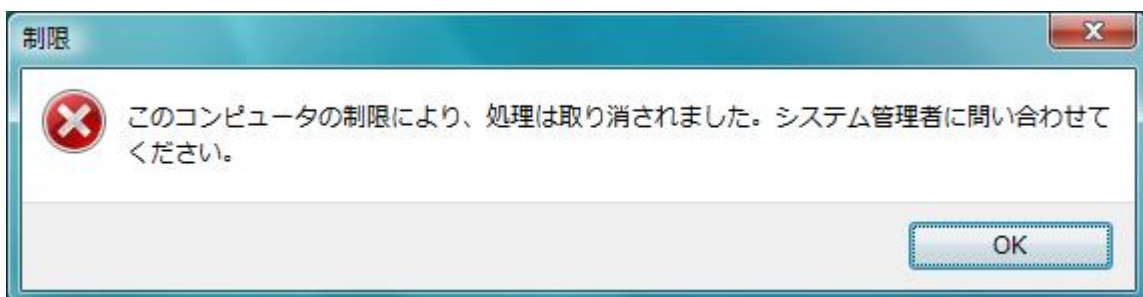
2.　下記の「その他のソフトウェア設定」画面が表示されますので、「追加」ボタンをクリックします。

＜その他のソフトウェア設定画面＞

3.　次の画面が表示されますので、追加する文字列を入力し「OK」ボタンをクリックすると、制限文字列が追加されます。

＜制限文字列の追加画面＞

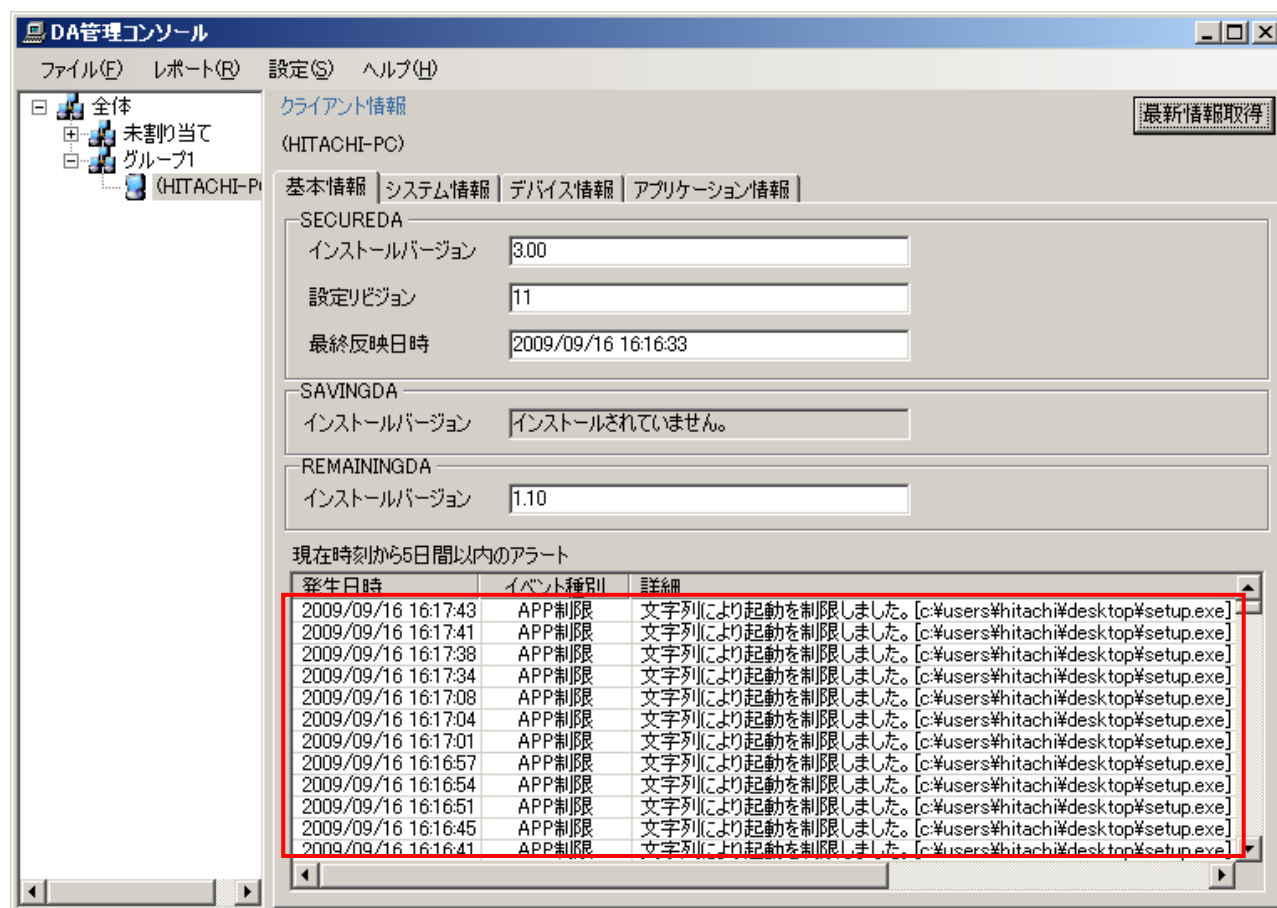
4.　「追加」した制限文字列をクリックして「編集」ボタンをクリック、または、「追加」した制限文字列をダブルクリックします。

＜その他のソフトウェア設定画面＞

5.　次の画面が表示されますので、制限文字列を編集してください。

＜制限文字列の編集画面＞

設定の反映の確認方法

制限したソフトウェアを実行した場合、以下のメッセージを表示してソフトウェアは実行できなくなります。

＜メッセージ画面＞

制限結果の確認方法

ソフトウェア制限を行い、制限したソフトウェアを起動した場合、アプリケーションの起動は制限されますが、ログは出力されません(一部、以下の画面のように出力する場合もあります)。

＜ソフトウェア制限画面＞

メニューバーの「レポート(R)」に結果レポート出力機能をサポートしています。

また、CSV 出力機能もサポートしていますので、用途に合わせてご利用ください。

ファイルアクセスを制限する

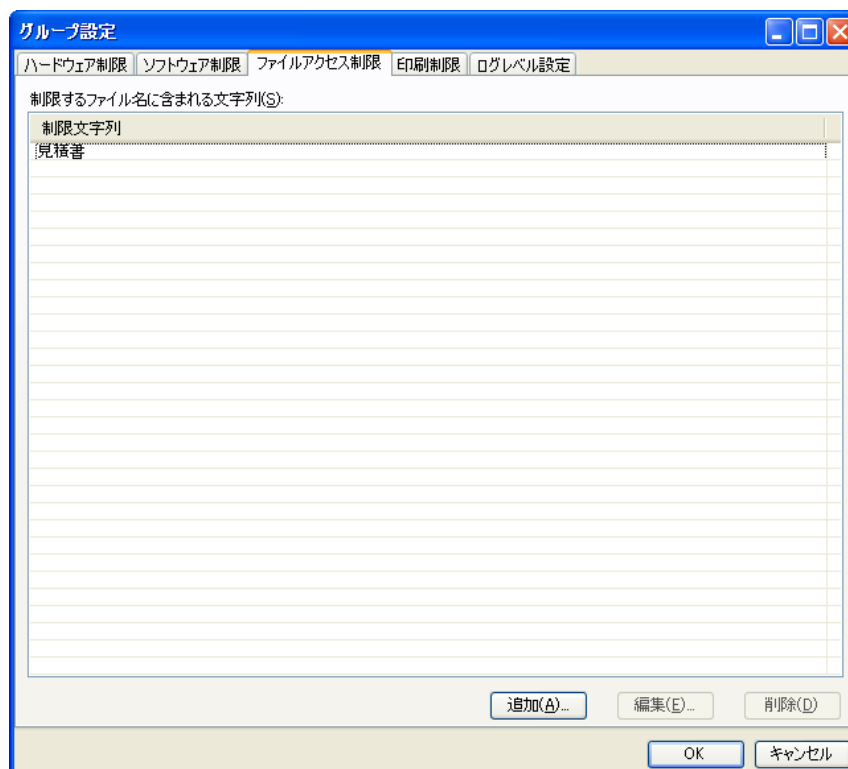
【注意事項】

- ファイルアクセス制限機能は Windows 7 では動作しません。

制限方法

指定文字列を含むファイル名のファイルへのアクセスを制限します。

機密文書などを登録しておき、閲覧/持出し等による情報流出を事前に防ぎます。

1. 制限するファイル名に含まれる文字列欄に、制限するファイル名を追加します。

＜ファイルアクセス制限画面＞

上記例の場合、ファイル名に”見積書”という文字列が含まれているファイルは全てアクセスが禁止されます。

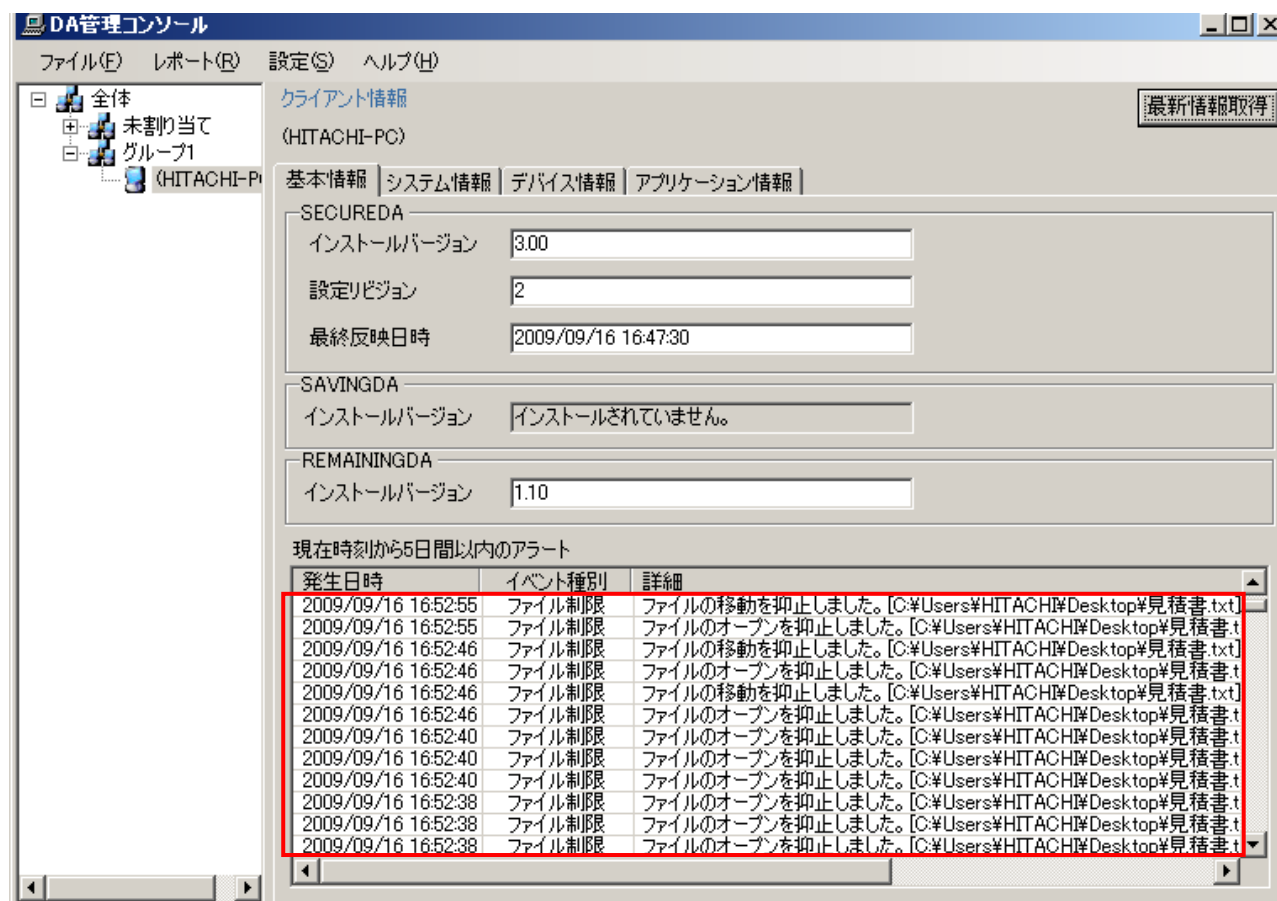
設定の反映の確認方法

ファイル名に指定した制限文字列が含まれるファイルのオープン、ファイルのコピー、ファイルのリネーム等すべてのファイルアクセスが禁止されます。
ファイルアクセスした場合、以下のようなメッセージを表示します。

＜メッセージ画面＞

注）ファイルアクセスするアプリケーションによって、メッセージが異なる場合があります。

制限結果の確認方法

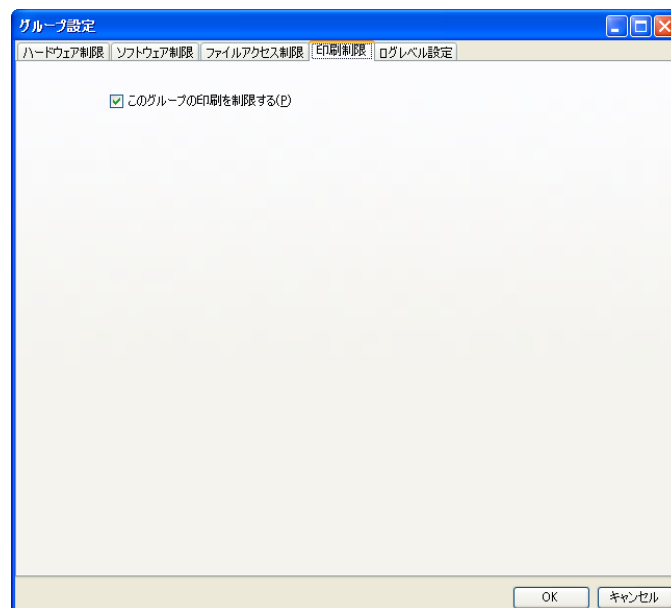
ファイルアクセス制限を行い、制限したファイルにアクセスすると、管理者用 PC のクライアント情報の「基本情報」画面に以下のように、「ファイルのオープンを抑止しました」または「ファイルの移動を抑止しました」とログが出力されます。

メニューバーの「レポート(R)」に結果レポート出力機能をサポートしています。

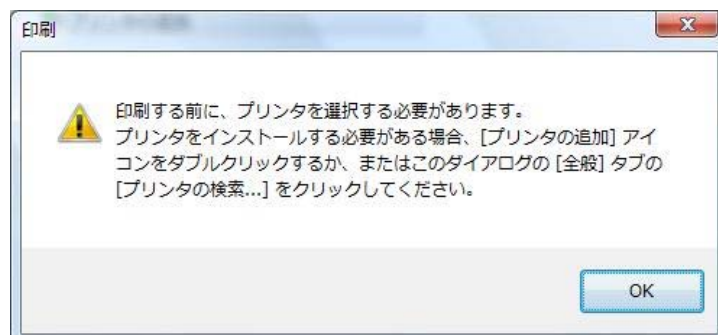
また、CSV 出力機能もサポートしていますので、用途に合わせてご利用ください。

印刷を制限する

制限方法

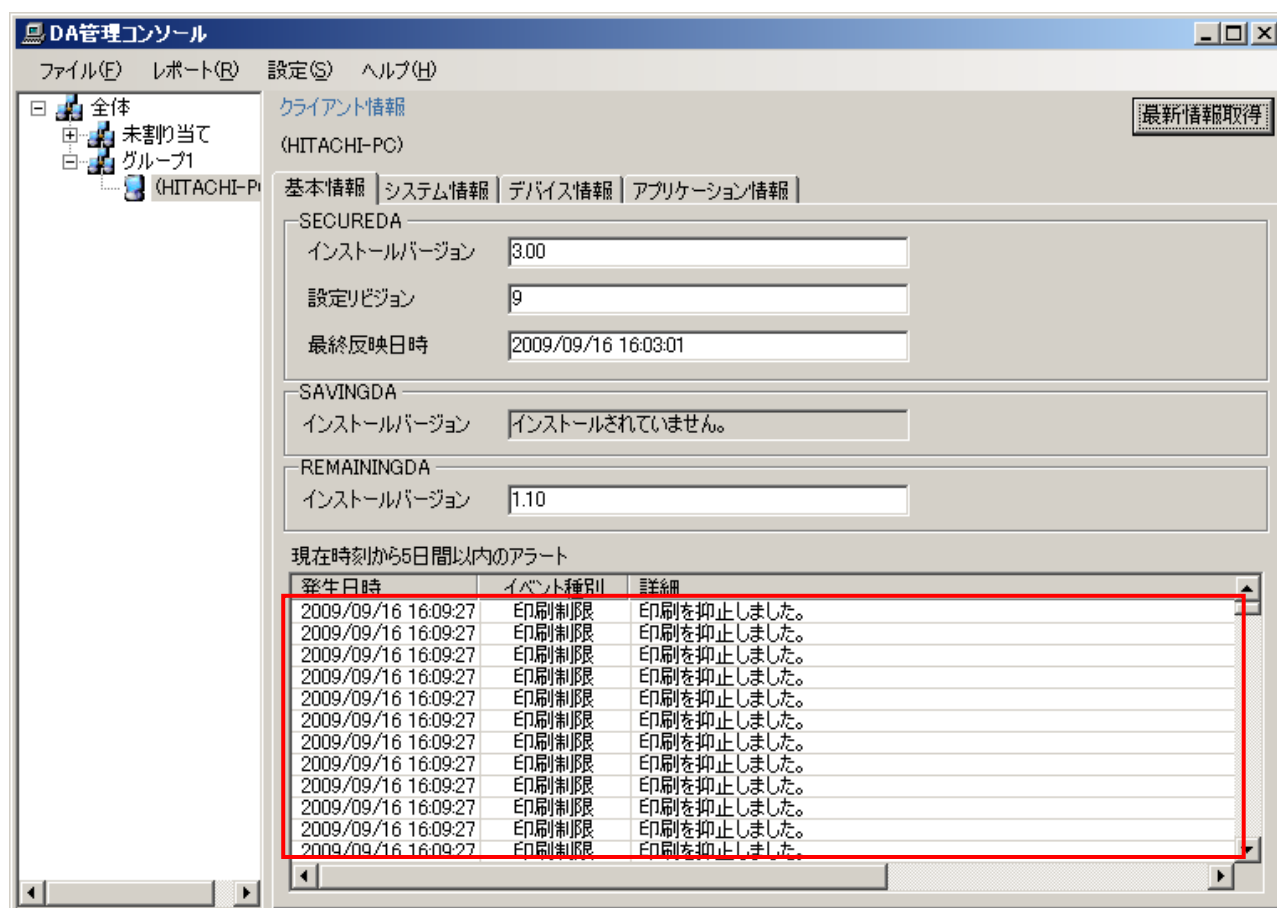
指定したグループの印刷を制限します。たとえば機密書類のプリントアウトを禁止できます。

1. 「このグループの印刷を制限する」チェックボックスをオンにします。

設定の反映の確認方法

印刷しようとした場合、以下のようなメッセージを表示します。

＜メッセージ画面＞

注） 印刷するアプリケーションによって、メッセージが異なる場合があります。

制限結果の確認方法

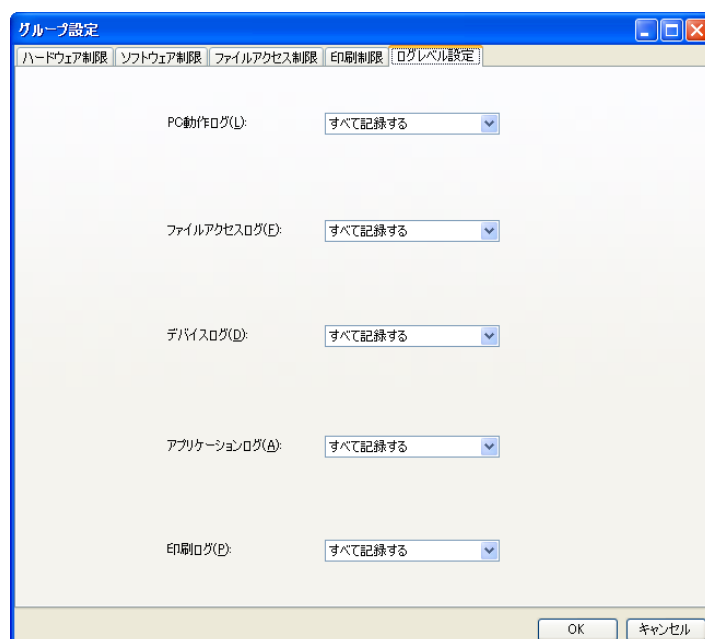
印刷制限を行い印刷を実行すると、管理者用 PC のクライアント情報の「基本情報」画面に以下のように、「印刷を抑止しました」とログが出力されます。

メニューバーの「レポート(R)」に結果レポート出力機能をサポートしています。

また、CSV 出力機能もサポートしていますので、用途に合わせてご利用ください。

ログレベルを設定する

設定方法

ログ出力時の動作を設定します。

設定内容を下記に示します。

＜ログレベル設定画面＞

ログ名称	設定内容
PC 動作ログ	記録しない／すべて記録する
ファイルアクセスログ	記録しない／アラートのみ記録する／すべて記録する
デバイスログ	記録しない／アラートのみ記録する／すべて記録する
アプリケーションログ	記録しない／アラートのみ記録する／すべて記録する
印刷ログ	記録しない／アラートのみ記録する／すべて記録する

- 記録しない：何も出力しません。
- アラートのみ記録する：アラート情報のみ出力します。
- すべて記録する：PC の起動/終了やユーザーのログオン/ログオフ等の動作ログも含む、すべてのイベント情報を出力します。

注）ファイルの「コピー」「移動」「削除」「名称変更」を行った場合、ご利用の OS によっては、ログに「ファイルオープン」と出力される場合があります。

また、Windows7 では、コピーや移動操作など、一部のファイルアクセスは記録できません。

設定結果の確認方法

ログレベル設定にて、アラートのみ記録する/すべて記録するを設定すると、管理者用 PC のクライアント情報の「基本情報」画面に以下のようにログが出力されます。

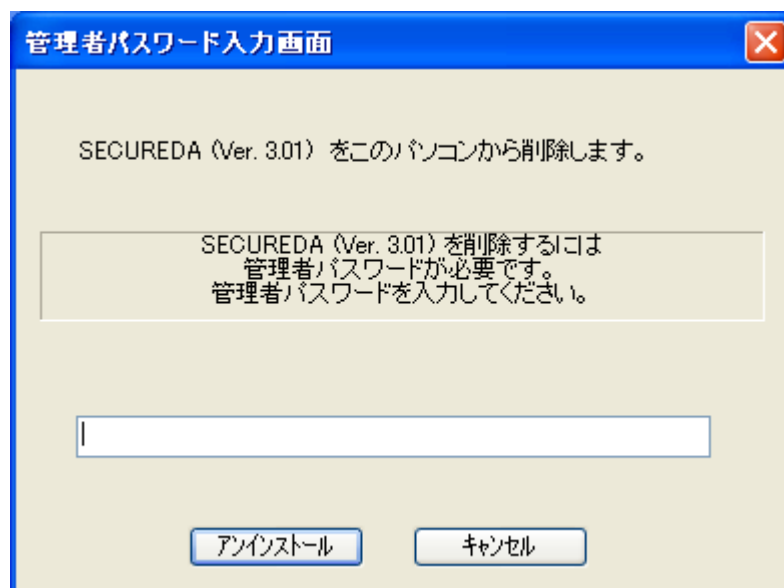
＜基本情報画面＞

SECUREDA Pro のアンインストール方法

SECUREDA Pro の使用を中止するなどシステムから削除する場合は、下記手順に従ってアンインストールを行ってください。

※重要:
クライアント PC に全ての制限を解除した制限設定を配布してから、クライアントソフトウェアのアンインストールを行ってください。特にプログラム名によるソフトウェアの実行制限はアンインストール後も有効となります。デバイス制限を適用したままクライアントソフトウェアをアンインストールしてしまった場合は、デバイスマネージャでデバイスを有効状態にしてください。

手順1. SECUREDA クライアントのアンインストール

1. クライアント PC に管理者権限を持つユーザーでログオンします。
2. 「SECUREDA Pro 管理用ソフトウェア」のインストールフォルダ内にある、SECUREDAPROUnInstall.exe をクライアント PC にコピーした後、実行します。
3. 管理者パスワードを入力してアンインストールを押してください。

＜クライアントのアンインストール画面＞

4. クライアント PC を再起動すれば、アンインストールは完了です。
   ※再起動を行うまで、クライアント PC にコピーした SECUREDAPROUnInstall.exe は削除しないでください。

(付録 1)SECUREDA 制限事項

No	カテゴリ	環境	内容	運用での対策方法
1	デバイス制限	全般	デバイス制限において、USB デバイスの取り外しに失敗する時がある。	対策方法なし。（制限事項）
2			USB デバイスのハブとホストコントローラが無効状態にされていると、USB デバイスが使用可能な制限設定を通知しても使用できない事がある。	対策方法なし。（制限事項）
3			デバイスログ出力の際、禁止操作を行っていないのに禁止操作を行った旨のログが出力されることがある。	対策方法なし。（制限事項）
4	アプリケーション 起動制限	全般	実行ファイルを「別の権限で実行」すると、アプリケーション起動制限が効かない。	対策方法なし。（制限事項）
5			スタートメニューのアクセサリからコマンドプロンプトを起動すると、アプリケーション起動制限が効かない。	アプリケーション起動制限機能を使う場合は、cmd.exe の使用を禁止してください。
6			16 ビットアプリケーションの起動・終了が、ログに出力されない。	対策方法なし。（制限事項）
7		WindowsVista Windows 7	実行ファイルを「管理者として実行」するとウィンドウタイトルに”管理者：～”と表示される。 管理コンソールでウィンドウタイトル制限の禁止文字列として”*管理者*”を登録しても、アプリケーションの起動制限が効かない。	アプリケーション起動制限機能は、エンドユーザーが管理者アカウントを持っていたり、権限を昇格してしまうと効かない場合があります。
8			実行ファイルを「管理者として実行」すると、アプリケーション起動制限が効かない。	アプリケーション起動制限機能を使う場合は、エンドユーザーには管理者アカウントを与えないようにしてください。
9			UAC（ユーザアカウント制御）の実行確認画面で、権限を昇格させて実行すると、アプリケーション起動制限が効かない。	

No	カテゴリ	環境	内容	運用での対策方法
10	アプリケーション起動制限	Windows 7	UAC（ユーザアカウント制御）の設定が“プログラムがコンピュータに変更を加えようとする場合のみ通知する”設定の時、アプリケーション制限が効かないことがある。	UAC の設定によっては管理者権限への昇格をユーザに確認せずに行う場合があり、管理者権限昇格したアプリケーションは起動の制限ができないため、管理者権限を必要としないアプリケーションが制限できていないように見えることがあります。 アプリケーション起動制限機能を使う場合は、エンドユーザーには管理者アカウントを与えないようにしてください。
11	ファイルアクセス制限	全般	16 ビットアプリケーションにファイルアクセス制限が効かない。	アプリケーション起動制限機能で ntvdm.exe を禁止にし、16 ビットアプリケーションを使えないようにしてください。
12		WindowsVista Windows 7	アクセス禁止にしているファイルに対して、コマンドプロンプトから edit コマンドを使用するとアクセスできてしまう。	アプリケーション起動制限機能で cmd.exe を禁止してください。
13		Windows 7	ファイルアクセス制限が機能しない。	Windows 7 ではファイルアクセス制限は機能しません。制限事項になります。
14	印刷制限	全般	16 ビットアプリケーションに印刷制限が効かない。	アプリケーション起動制限機能で ntvdm.exe を禁止にし、16 ビットアプリケーションを使えないようにしてください。